Intelligence Driven Malware Analysis (IDMA)
Malicious Profiling

14 January 2015

Homeland Security

National Cybersecurity and
Communications Integration Center

whoami

- Cyber Threat Analyst at Northrop Grumman
    - Performed wide range of duties from malware analysis to cyber threat reporting
    - Supporting US-CERT/NCCIC
- B.S. in Digital Forensic Science from Defiance College (Ohio)
- M.S. in Digital Forensic Science from Champlain College (Vermont)
- Certifications
    - GIAC Certified Reverse Engineer of Malware (GREM)
    - GIAC Certified Incident Handler (GCIH)
    - GIAC Certified Forensic Analyst (GCFA)

Outline

- Introduction & Purpose
- Foundation & Origin
- IDMA Overview
- Critical Components
- Operational Use Case
- Conclusions

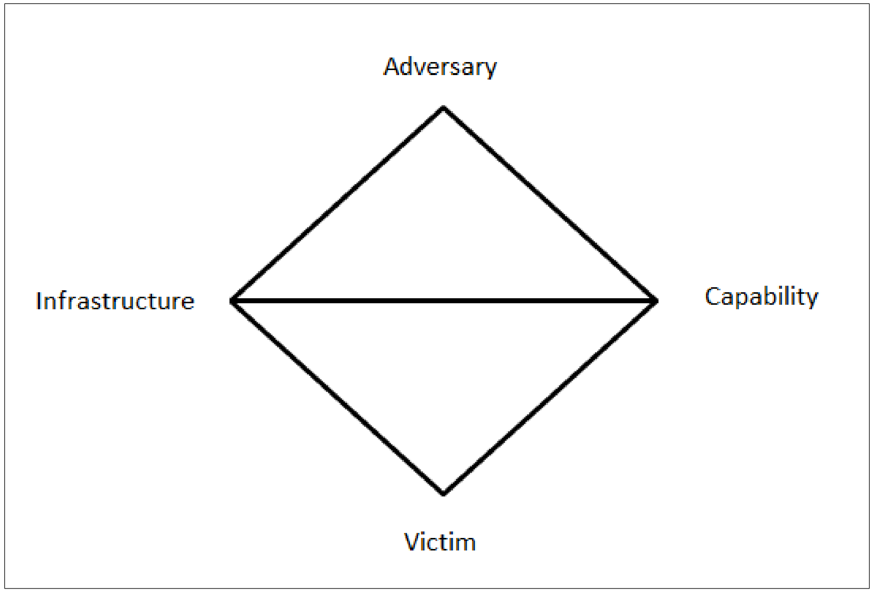
Introduction & Purpose

- Malware Analysis Integration
  - Reduce operational isolation
  - Increase effectiveness of threat intelligence and incident response operations
- Augment Existing Methodologies
  - Not attempting to reinvent the wheel
  - Utilize threat intelligence to drive analysis

Foundation & Origin

- Diamond Model of Intrusion Analysis *(Caltagirone et al. 2013)*
- Robust and Scalable
  - Designed for incident response
  - Adapted for malware analysis

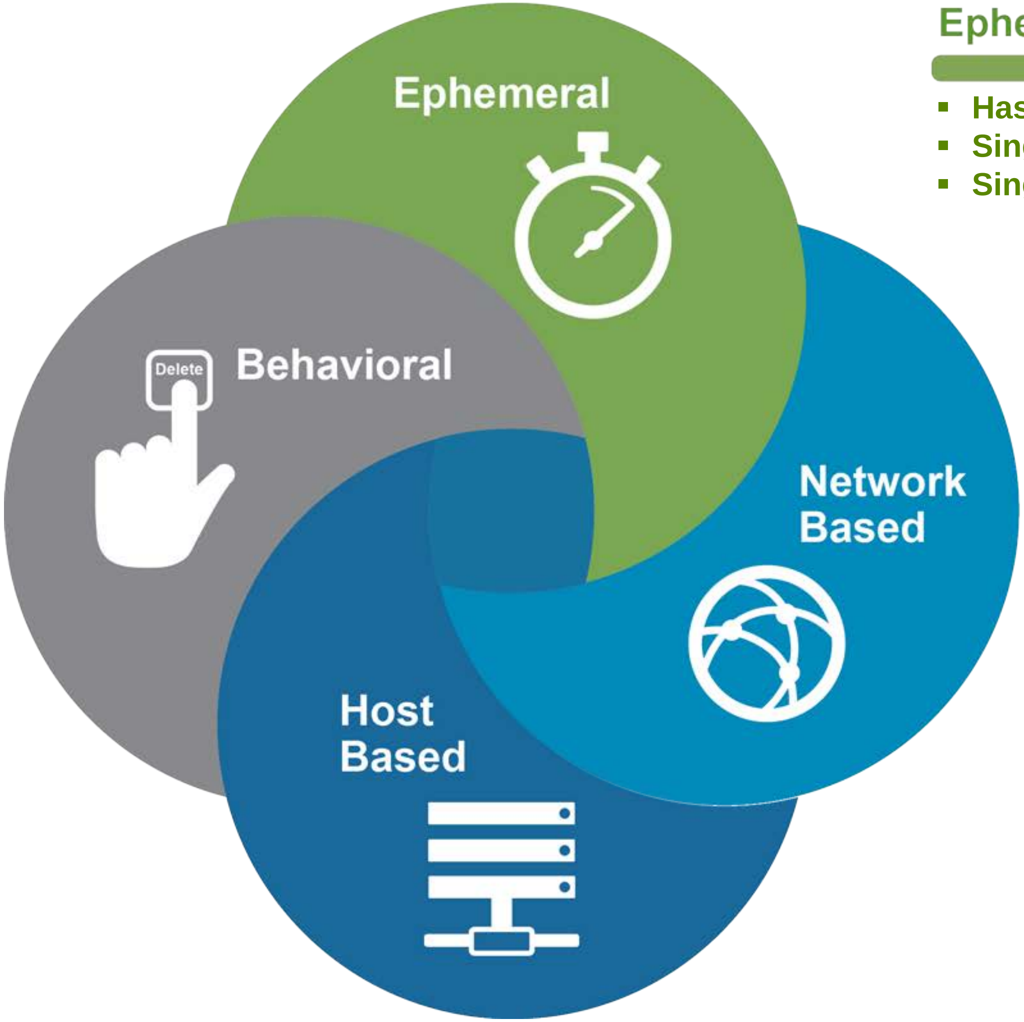
- Facilitate a Bridge
  - Incident response
  - Malware analysis
  - Threat intelligence



Critical Components of IDMA

- Indicator Classification
  - Novel concept
  - Provides context for analysis
- Indicator Correlation
  - Novel concept
  - Facilitates actionable and relevant indicators
- Threat Intelligence Order of Volatility (TI-OV)
  - Novel concept
  - Methodical order of precedence

Indicator Classification & Correlation



Ephemeral

- Hash values
- Single IP address
- Single domain

Network Based

- Source and destination IP (net flow)
- Targeted ports and services
- Beacon addressed and locations
- Delivery methods

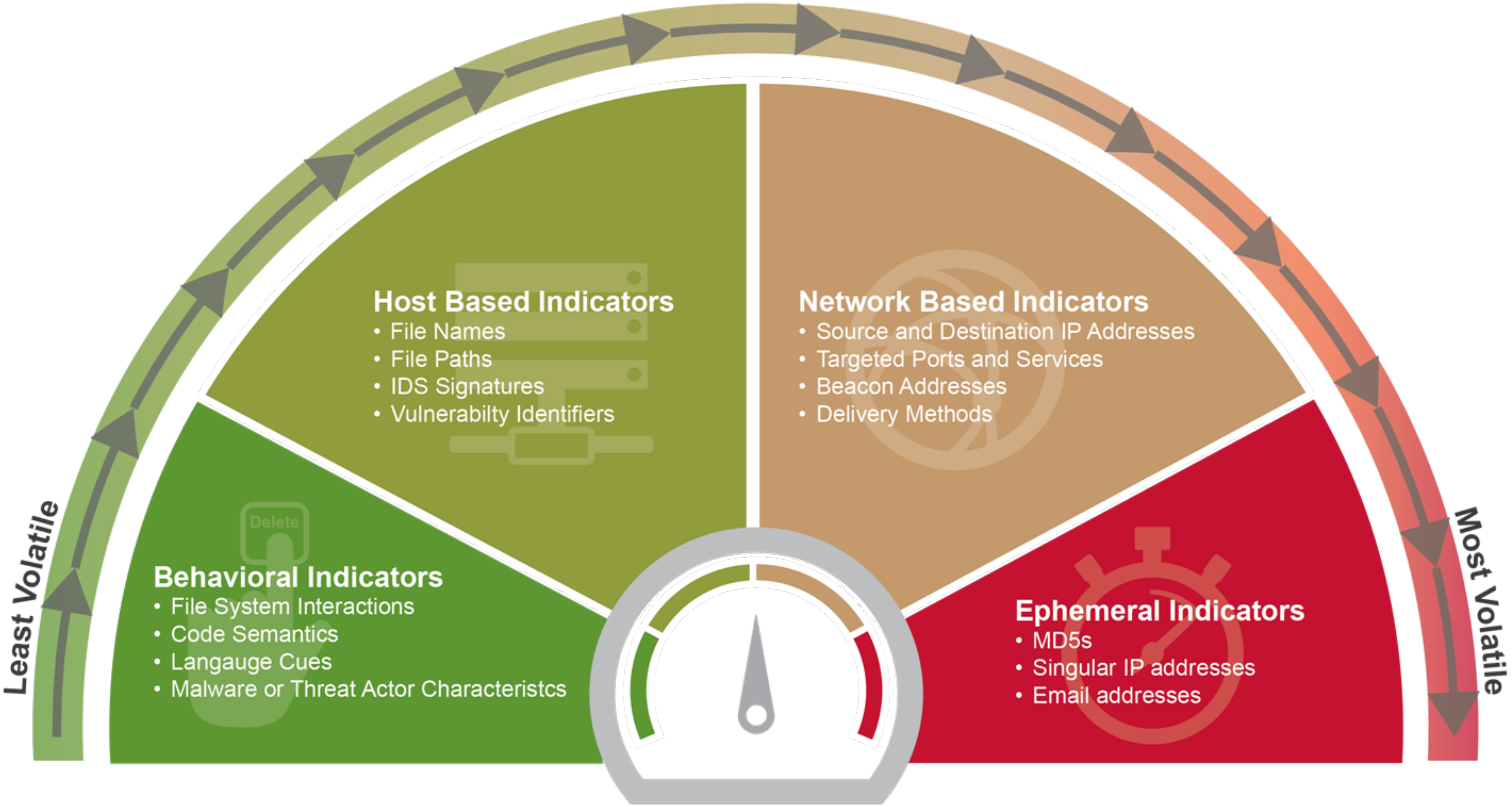
Host Based

- File names
- File paths
- IDS signatures or other detection methods
- Intrusion objectives (if known)
- Vulnerability identifiers

Behavioral

- File system interaction (create, change, delete)
- Registry interactions
- Toolchain analysis (packer, compiler)
- Impact and outcome

Threat Intelligence Order of Volatility (TI-OV)



Behavioral Indicators
- File System Interactions
- Code Semantics
- Langauge Cues
- Malware or Threat Actor Characteristcs

Host Based Indicators
- File Names
- File Paths
- IDS Signatures
- Vulnerabilty Identifiers

Network Based Indicators
- Source and Destination IP Addresses
- Targeted Ports and Services
- Beacon Addresses
- Delivery Methods

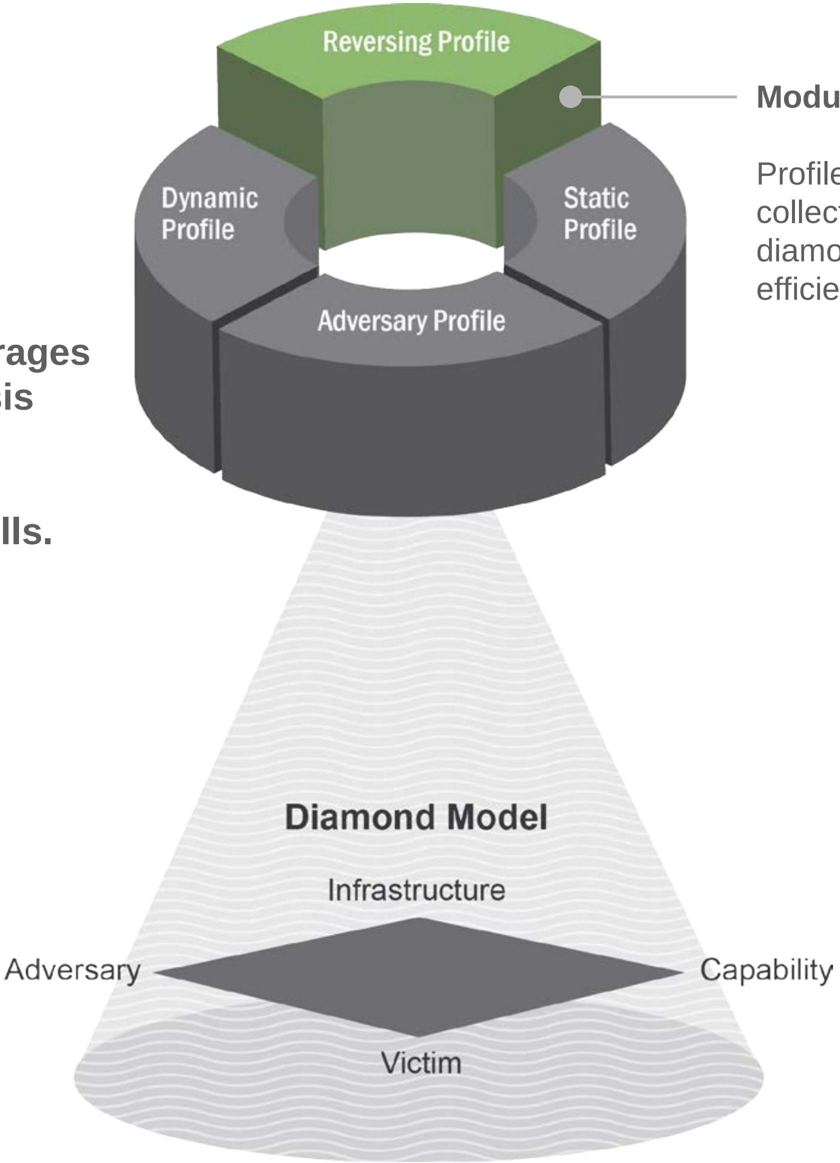
Ephemeral Indicators
- MD5s
- Singular IP addresses
- Email addresses

Profiles of Analysis

- Four Core Profiles (Analysis Methods)
  - Static, Dynamic, Reversing, Adversary
- Segmented Analysis
  - Reinforce existing methodologies
  - Multiple components = one profile
  - Modular system of analysis
- Critical Questions of Malicious Profiling
  - Provides focus to core profiles
  - Drives analysis towards intelligence criteria

IDMA Profiles

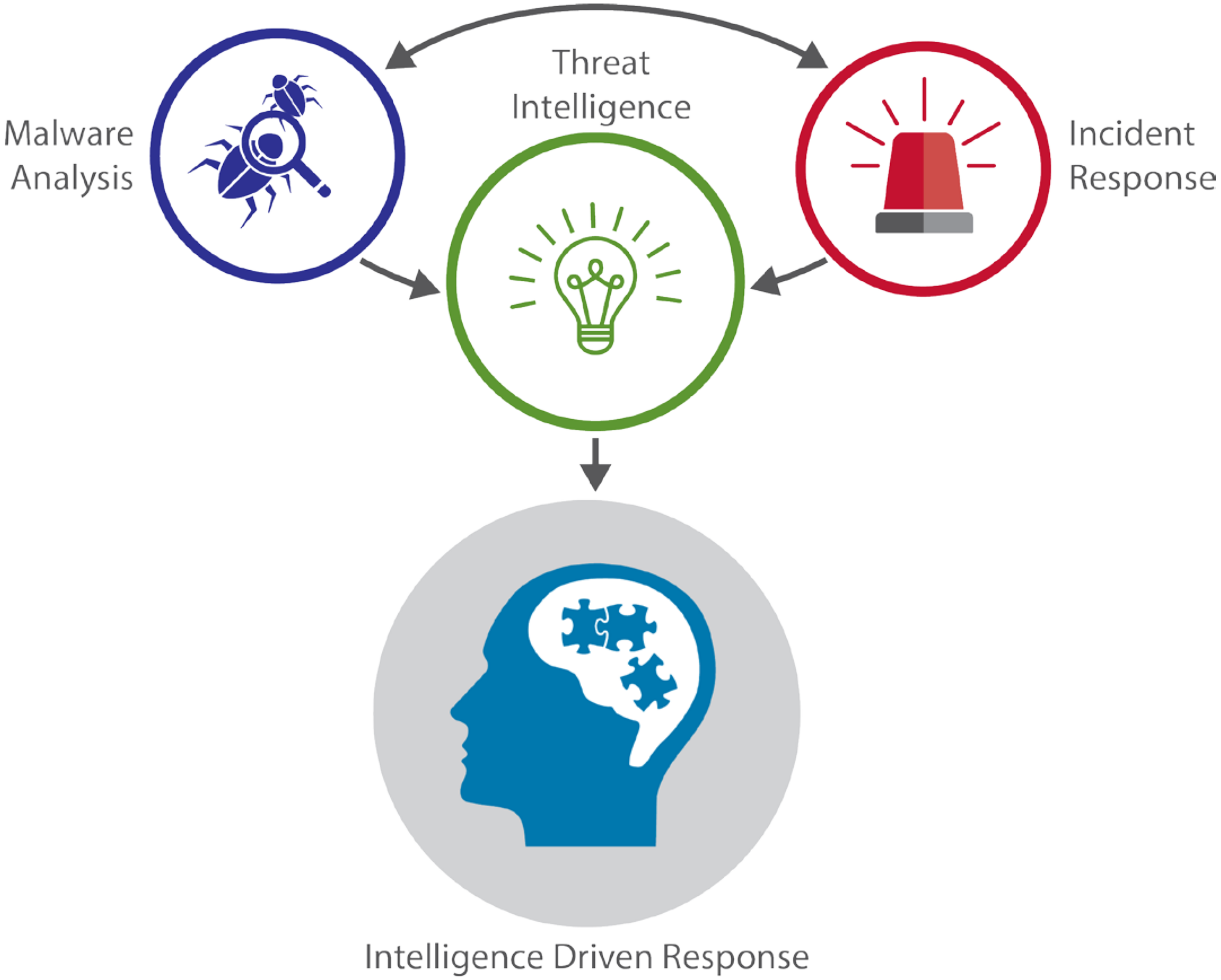
The basic concept of malicious profiling leverages existing malware analysis techniques applied with critical thinking and intelligence analysis skills.



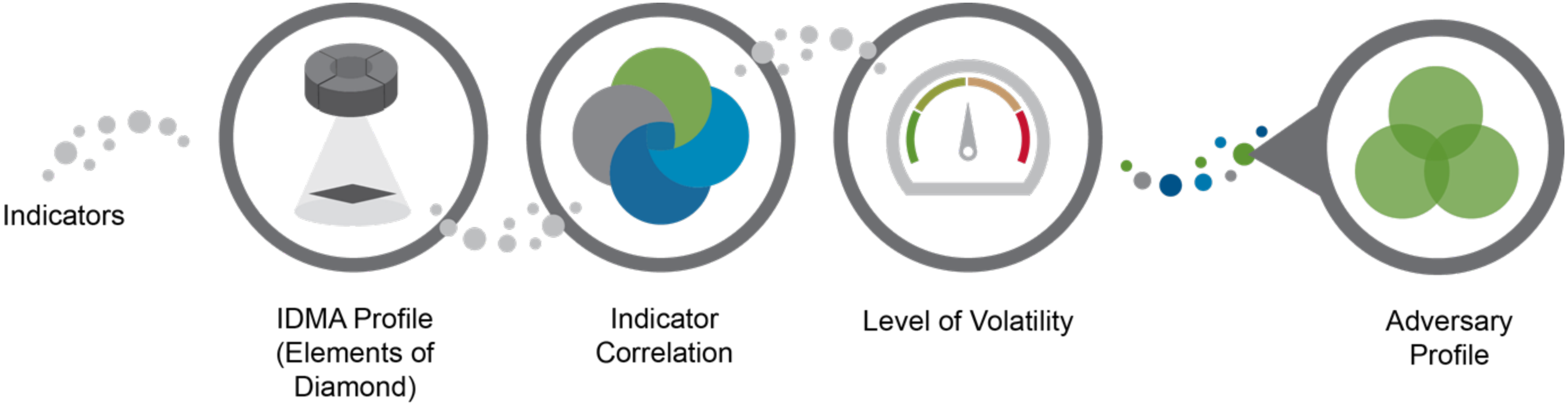
Modular analysis

Profiles can be individually or collectively applied to the diamond model to increase efficiency and focus analysis.

IDMA Concept



IDMA Process Flow



Indicators

IDMA Profile (Elements of Diamond)

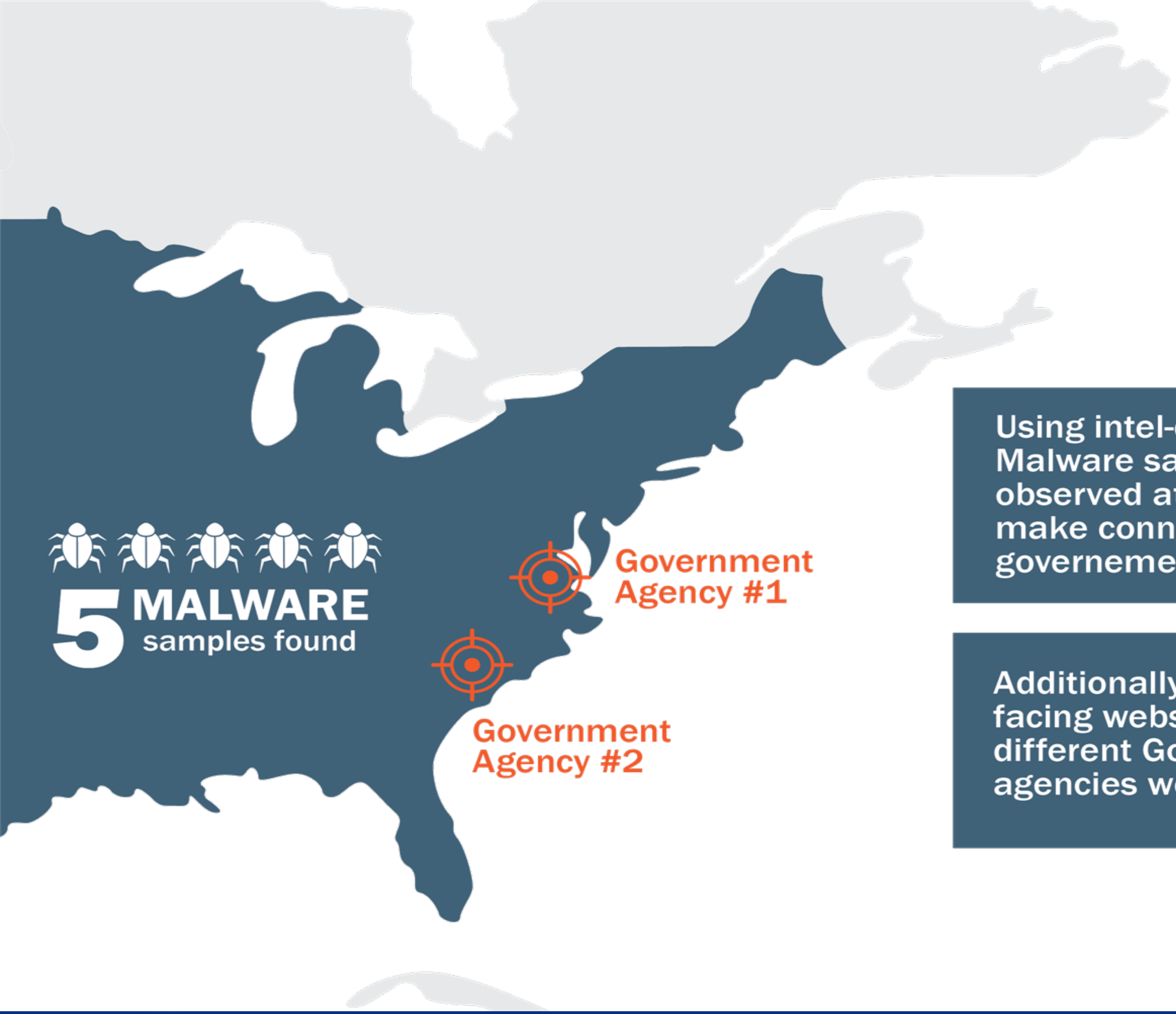
Indicator Correlation

Level of Volatility

Adversary Profile

Use Case

- SATR Discovery
  - Malware hashes beaconing to government hosts
  - Intelligence -> malware analysis -> incident response
- IDMA Analysis
  - Integration of efforts
  - IDMA project was a derivative of this effort



Using intel-driven data, Malware samples were observed attempting to make connections to governement machines

Additionally, two external facing websites from two different Government agencies were identified

Use Case: Malicious Profile

TI-OV		Adversary	Infrastructure	Capabilities	Victim
🟩	Behavioral	Anti-forensic techniques		Sample signed with two digital certificates	
🟨	Host Based				Public facing server URL Designed to run on Windows XP
🟫	Network Based	Digital certificate domains	Malicious domain hardcoded		Hosting IP address
🟥	Ephemeral	Compile time		Sample hash	Detection Time

(Zeltser, 2015)

Use Case: Correlating Evidence

- Original Work Flow
  - Samples discovered
  - Net flow examined (limited scope)
  - Samples were sent to malware shop (little context provided)
    - Callback domain
    - Net flow conclusions
  - Total time invested ~10 days (prior to additional response)
- IDMA Work Flow
  - Samples discovered
  - IDMA applied (context discovery)
  - Samples can be sent to malware shop
    - Indicators from all 8 categories of the profile supplied
  - Additional context can drive further analysis (malware, IRT)

Use Case: Correlating Evidence

- Original Work Flow
  - Samples discovered
  - Net flow examined (limited scope)
  - Samples were sent to malware shop (little context provided)
    - Callback domain
    - Net flow conclusions
  - Total time invested ~10 days (prior to additional response)

- IDMA Work Flow
  - Samples discovered
  - IDMA applied (context discovery)
  - Samples can be sent to malware shop
    - Indicators from all 8 categories of the profile supplied
  - Additional context can drive further analysis (malware, IRT)

Use Case Conclusions

- Full Scale Reverse Engineering
    - Time consuming, resource intensive process
    - Few individuals are fully qualified
- IDMA Analysis
    - Two profiles used (Static, Reversing)
    - Tools utilized
        - OllyDbg
        - PEStudio
        - BinText
    - Context driven analysis
    - Total time invested ~3 hours (additional)

Conclusions

Context

- Shift field away from single indicators
- Additional context increases effectiveness of incident response and threat intelligence operations

Volatility

- Facilitates indicator precedence
- Focus analysis on less volatile indicators
- Adds additional context for reporting

Malware Analysis & Diamond Model

- Sample analysis can feed all four components
- Malware analysis does not have to be compartmentalized & segregated

Value of Time

- Context and behavior can be derived without full scale reversing
- Can lead to increased effectiveness in incident response operations

Questions?